

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 1405.1020

First Named Inventor or Application Identifier:

Hideyuki HIRANO et al.

Express Mail Label No.

jc658 U.S. PTO

09/559259



04/27/00

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
2. ☒ Specification, Claims & Abstract [Total Pages: 29]
3. ☒ Drawing(s) (35 USC 113) [Total Sheets: 8]
4. ☒ Oath or Declaration [Total Pages: 4]
 - a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 17 completed)
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation by Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy (identical to computer copy)
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☒ Information Disclosure Statement (IDS)/PTO-1449 ☒ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☐ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ☐ Small Entity Statement(s) ☐ Statement filed in prior application, status still proper and desired.
15. ☒ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Other:

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: /

18. CORRESPONDENCE ADDRESS

STAAS & HALSEY LLP
Attn: James D. Halsey, Jr.
700 Eleventh Street, N.W., Suite 500
Washington, DC 20001

Telephone: (202) 434-1500
Facsimile: (202) 434-1501

TITLE OF THE INVENTION

DATA MANAGEMENT METHOD

BACKGROUND OF THE INVENTION

Technical Field

5 The present invention relates to data management methods; particularly, it relates to data management methods wherein digital content is encrypted with special access information and distributed.

Description of Related Art

10 Electronic data in computer program software and electronic publishing materials is vended stored on magneto-optical disks (MO), digital video disks (DVD), floppy disks (FD), mini disks (MD) and other recording media. Electronic data thus is generally easy to copy, and illicit copies are
15 frequently made. That copyrights on the software vendor and publisher end will be infringed and considerably hinder profits is therefore a worry.

 The situation is the same with electronic data containing still image data and motion picture data
20 distributed via the Internet, CATV and other networks: illicit copies are made frequently, consequently damaging copyright holders' profits.

 For protecting so-called digital content, such as electronic data stored on the recording media described
25 above and electronic data distributed via the variety of

networks, it has been the practice to encrypt the digital content using an encryption key, and the thus distributing the substantive data that has been encrypted.

Assuming, for example, that a user accesses a content distributor from his or her own personal computer, then
5 downloads the digital content onto a hard disk, and thus uses the digital content: To start with, the user accesses a host computer and obtains a plug-in module for downloading. Thereafter, the user forwards, to the host
10 computer, an in-use hard disk drive identification number, an in-use computer CPU identification number, and other identification information items unique to the user.

On the content distributor end, substantive data in which digital content is encrypted with a content key and
15 authorization information in which the content key is encrypted with user-specific identification information, is sent to the user end.

On the user end, the encrypted substantive data that has been sent and the authorization information are recorded
20 as is encrypted on the hard disk. When using the digital content, employing user-specific identification information such as the hard disk drive identification number, the authorization information is decrypted and the content key is thereby obtained. The digital content is decrypted with
25 the content key and thus used.

Herein, when granting individual users the right to use the digital content, the encryption key for encrypting the digital content can be made common, and use privileges can be granted individually to users by encrypting a decryption
5 key utilizing user-specific information different for every user.

Wherein data is distributed by the methods described above, the data distributor is required to forward separately the encrypted digital content and the
10 authorization information serving as the decryption key for the encrypted digital content.

Further, on the user end, the encrypted digital content and the authorization information that have been forwarded have to be stored separately on the recording medium.

15 Consequently, if the authorization information is damaged during the course of being forwarded to the user end from the data distributor end, or if the authorization information is otherwise damaged or lost due to some mishap on the recording medium on the user end, the digital content
20 will become unusable. This makes it necessary to go through a process for acquiring second-time authorization information.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a data
25 management method that by encrypting and distributing

digital content prevents copyright infringement, and that prevents authorization information for decrypting the encrypted digital content from being damaged or otherwise lost.

5 A data management method according to the present invention comprises a step of preparing a substantive data file by encrypting a digital content to be distributed, a step of extracting a part of the digital content as sample data, and preparing sample data file by embedding, into the
10 sample data, authorization information as invisible information containing information on a content key used as an encryption key when encrypting the digital content, and a step of preparing synthesized data by synthesizing the substantive data file with the sample data file.

15 When using the distributed digital content, this involves separating the authorization information from the sample data file, restoring the content key for decrypting the substantive data file from the authorization information, and decrypting the substantive data file into
20 the original digital content by use of the content key for its use.

 With this contrivance, the substantive data file is integrally synthesized with the authorization information embedded as the invisible information into the sample data
25 file, thereby preventing a breakage and a loss of the

authorization information for decrypting the substantive data file. The data of the digital content can be distributed by circulating the synthesized data, whereby the system can be downsized.

5 The sample data may be image data contained in the digital content, on which at least one of image processing, resizing, compressing and a γ -compensation is executed.

Further, the sample data may be index data representing the substantive data file.

10 Further, the synthesized data may contain a plurality of substantive data files based on a plurality of digital contents, a plurality of sample data files corresponding to the plurality of substantive data files, and each of the sample data constituting the plurality of sample data files
15 may be linked to the corresponding substantive data file among the plurality of substantive data files.

Moreover, the sample data file may be defined as structured data based on JPEG (Joint Photographic Experts Group) and MPEG (Motion Picture Experts Group), and the
20 synthesized data may be prepared by additionally synthesizing the substantive data file with the sample data file by use of a format of the sample data file.

The authorization information may be what the content key is encrypted in such a way that at least one of user
25 identification information, identification information on a

device incorporated into a computer employed by the user,
identification information on a CPU mounted in the computer
employed by the user and identification information peculiar
to a recording medium for storing the digital content,
5 serves as an encryption key. Further, the authorization
information may also be what the content key is encrypted,
with identification information common to a plurality of
users serving as an encryption key. In addition, the
authorization information may be what the content key is
10 encrypted in such a way that at least one of identification
information unique to a distributor of the digital content
and identification information unique to an author of the
digital content, serves as an encryption key.

The decryption key for decrypting the encrypted
15 content key is common to the encryption key for executing
the encryption, and may be a common key based on unique
information transmitted and received between the user and
the content distributor.

The distributor of the digital content may encrypt the
20 content key by use of a secret key, and the user may decrypt
the encrypted content key by use of a public key provided
beforehand from the distributor of the digital content.

Furthermore, the sample data file may contain the
number of times as invisible information with which the user

uses the digital content, and the invisible information may be rewritten each time the user uses the digital content.

The sample data file may further contain authorization information as invisible information which makes it feasible
5 to control the number of uses, and the invisible information may be rewritten when the user uses the digital content over a predetermined number of times.

In that case, the invisible information may be rewritten when reading the substantive data file after
10 decrypting the same data file or when the use of the digital content is finished.

The invisible information of the sample data file contains redundant information and thereby incorporates an error recovery function.

15 The system may be constructed so that a range of regeneration based on the invisible information of the sample data file is regulated when decrypting the substantive data file. A range of any one category of years, months, dates and hours for which the regeneration
20 can be done based on the invisible information of the sample data file is regulated when decrypting the substantive data file.

From the following detailed description in conjunction with the accompanying drawings, the foregoing and other
25 objects, features, aspects and advantages of the present

invention will become readily apparent to those skilled in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic configurational diagram of the present invention;

Fig. 2 is a schematic diagram of the configuration on the content administrator end;

Fig. 3 is a schematic diagram of the configuration on the content user end;

Fig. 4 is a theoretical depiction of an instance of content distribution;

Fig. 5 is a flowchart of an instance of content distribution;

Fig. 6 is a theoretical depiction of an instance of content use;

Fig. 7 is a flowchart for an instance of content use;

Fig. 8 is an explanatory diagram illustrating JPEG data structure; and

Fig. 9 is a configurational diagram illustrating an example of a management mode.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Outline of the Invention

Fig. 1 shows an outline of architecture according to the present invention.

A content provider 1 may be an author and a copyright holder of digital contents, and provides a content administrator 2 with a digital content 11 to be operated.

The content administrator 2 encrypts, for its
5 operation, the digital content 11 provided from the content provider 1. The content administrator 2 manages an encryption key thereof and also manages user information of a user who utilizes the digital content 11.

A content user 3, when trying to use the digital
10 content managed by the content administrator 2, transmits user information 14 to the content administrator 2.

The content administrator 2 manages the user
information 14 transmitted from the content user 3, prepares content use authorization information 13 based on this item
15 of user information 14, and transmits the authorization information 13 combined with an encrypted content 12 to the content user 3.

In this case, the content administrator 2 extracts such sample data as to represent its substance out of the
20 digital content 11. The content administrator 2 encrypts the encryption key, by which the digital content 11 has been encrypted, with the user information 14, thereby preparing the content use authorization information 13. The content administrator 2 prepares a sample data file by embedding the
25 authorization information 13 as invisible information into

the sample data. Further, the content administrator 2 synthesizes this sample data file with the encrypted content 12, and transmits the synthesized content to the content user 3.

5 In that case, the content provider 1 may be identical in function with the content administrator 2.

Content administrator

Reference is made to Fig. 2, a functional block diagram schematically depicting configuration on the content administrator 2 end. The system on the content administrator 2 end includes: a content administration module 21 for managing the content to be run; a content encryption unit 22 for encrypting the digital content by use of predetermined content keys; a content key administration unit 23 for administering content keys; a user information administration module 24 for obtaining the user information from a content user 3 and administering this item of user information; an authorization information administration module 25 for preparing user authorization information for the digital content on the basis of the user information administered by the user information administration module 24 to administer the information; a authorization-information-embedded sample preparing unit 26 for extracting sample data from the digital content and embedding the authorization information as invisible information into the

10
15
20
25

sample data; and an encrypted content synthesizing unit 27 for synthesizing the authorization information embedded sample data with the encrypted content encrypted by using the content key.

5 *Content User*

Reference is made next to Fig. 3, a functional block diagram schematically showing a configuration on the side of the content user 3.

The system on the content user 2 end includes: a user
10 information administration module 31 for managing
identification numbers of in-use hard disk drives; an
identification number of a CPU incorporated into a computer
and other items of identification information unique to
users; a synthesized data acquisition unit 32 for acquiring
15 synthesized data from the content administrator 2; a sample
data display unit 33 for displaying sample data from the
acquired synthesized data; an authorization information
extracting unit 34 for separating the authorization
information from the authorization-information-embedded
20 sample data; a content key decryption unit 35 for
regenerating the content key by decrypting the extracted
authorization information; a content decryption unit 36 for
decrypting the encrypted content by use of the decrypted
content key; and a content running unit 37 for running the
25 decrypted digital content.

Distribution of Content

An operation performed by the content administrator 2 when distributing the digital content will be described based on Fig. 4 and 5.

5 The digital content 11, into which content information 42 thereof is embedded as a watermark, turns out to be a watermarked content 43. Herein, the content 11 may be structured so that the content information 42 is inserted into a specified frequency band of the data, and may also be
10 structured so that a part of the data is thinned out and the content information 42 is inserted therein. The content information 42 may be set as, e.g., information on the copyright of the digital content 11, and the embedding of such an item of information may be omitted.

15 In step S1, the watermarked content 43 is encrypted by use of a content key 44, thereby preparing an encrypted content 45.

 The user information 14 is acquired in step S2. Herein, if accessed from the content user 2, items of
20 identification information unique to the content user 3 such as the identification number of the hard disk drive used by the content user 2 and the identification number of the CPU mounted in the computer, are transmitted and stored in the user information administration module 24 (see Fig. 2).

In step S3, the content key 44 is encrypted by using the acquired user information 14, and a secret key 46 is prepared. This secret key 46 is encrypted based on the user information 14 unique to the content user 3, and therefore
5 serves as authorization information by which the digital content 11 is allowed to be used.

Data representing the content is extracted as sample data 41 out of the digital content 11 in step S4. If the digital content 11 contains plural items of image data, one
10 item of image data among them may be extracted as the sample data 41. In the case of simultaneously operating the plurality of digital contents 11, the system can be constructed so that the sample data 41 extracted herein is linked to the digital content 11 corresponding thereto, and
15 a desired item of sample data among plural items of sample data is selected, thus choosing the digital content to be used.

In step S5, the secret key 46 is embedded as a watermark into the sample data 41, thereby preparing
20 watermarked sample data 47. The watermarked sample data 47 may be, as in the manner described above, structured so that the data of the secret key 46 is inserted into a specified frequency band of the data, and may also be structured so that a part of the data is thinned out and the data of the
25 secret key 46 is inserted therein. With this design, it

follows that there is prepared the authorization information embedded sample data into which the authorization information is embedded as invisible information.

Synthesized data 48 is prepared by synthesizing the encrypted content 45 with the watermarked sample data 47 in step S6.

In a case where the digital content 11 is composed of plural items of image data, the data may be distributed by setting the sample data in a structured data format based on a standards group such as JPEG (Joint Photographic Experts Group). In this case, the sample data 41 is paired with the digital content 11, and the authorization information is embedded therein per content, thus preparing the watermarked sample data 47. Then, the digital content 11 is additionally synthesized with the sample data 47.

Fig. 8 shows a JPEG data structure in that case. The watermarked sample data 47 is structured as a sample data file 61 consisting of a Start Of Image (SOI) point 63, an End Of Image (EOI) point 65, and a frame 64 interposed between the start point 63 and the end point 65. Further, a substantive data file 62 is configured by a digital content 66 encrypted by the content key 44, and this sample data file 61 and the substantive data file 62 are integrally synthesized.

0024015265300

In step S22, a watermarked sample data **50** in the synthesized data **48** is displayed. If the synthesized data **48** contains a plurality of digital contents, items of watermarked sample data **47** corresponding to the respective
5 digital contents may be arranged in reduction and sequentially displayed by scrolling and switching, whereby a catalog display function can be given. Software of a client may be provided with this kind of function. Even when only one digital content exists within the synthesized data **48**,
10 the system may also be constructed so that the sample data file is structured by extracting some items of sample data and displayed in catalog. As a matter of course, in the case of a single item of sample data, the system may be constructed so that the single data is displayed as it is.

15 It is judged in step S23 whether or not there is a use request given from the content user **3**. When the content user **3** selects a specified item of sample data and gives an indication of using the same data on the display of the watermarked sample data **50**, the process flow goes to step
20 S24, in which content using software is operated.

The authorization information is separated from the watermarked sample data **47** in the synthesized data **48** in step S24. Herein, the secret key **46** embedded as a watermark into the watermarked sample data **47**, is de-embedded. If the
25 secret key **46** is embedded as a frequency component of the

sample data, the secret key 46 can be de-embedded by analyzing the frequency of the watermarked sample data 47. Further, in the case of implementing physical embedding such as embedding the watermark after thinning out the sample data, the secret key 46 can be de-embedded by performing an image analysis.

In step S25, the de-embedded secret key 46 is decrypted by use of the user information 14, the content key 44 is regenerated.

In step S26, the encrypted content 45 is decrypted by use of the regenerated content key 44, and the watermarked content 43 is developed on the hard disk and/or IC memory.

The content is utilized by actually operating the watermarked content 43 in step S27.

Mode of Data Operation

An operation mode as shown in Fig. 9 may be taken.

A content provider 51 may be an author and a copyright holder of digital contents, and provides a content administrator 52 with a digital content (A).

The content administrator 52 encrypts the digital content provided from the content provider 51 by use of a content key.

The content administrator 52 transmits the encrypted digital content and the content key to a center 53 for actually distributing the data (B). The center 53 manages

the encrypted digital content and the content key. The center 53 may be a WEB server within the Internet and a variety of other networks, and is constructed so as to distribute the digital content in response to access from a user 54.

The user 54 accesses the center 53 via a WEB browser, and acquires a plug-in module for obtaining the data (C). The user 54 starts up the plug-in module on the WEB browser, and forwards to the center 53 identification information unique to the user such as an identification number of the hard disk drive employed by the user himself or herself (D).

The center 53 prepares the authorization information by encrypting the content key on the basis of the identification information unique to the user, and embeds the authorization information as a watermark into the sample data of the digital content. The center 53 then prepares a authorization information embedded encrypted content by synthesizing the sample data with the encrypted content. The center 53 transmits the authorization information embedded encrypted content to the content user 54 (E).

The content user 54 stores the received authorization information embedded encrypted content in a user's disk 55 such as a hard disk (F).

When utilizing the digital content, the content key is taken out of the authorization information embedded

encrypted content stored in the user's disk 55 by use of the identification information unique to the user (G), and decrypts the encrypted content by the content key, thus taking out the digital content (H).

5 Such a system architecture being thus made, there is no necessity for changing the content key for encrypting the digital content for every content user, and one single content key suffices for one digital content, thereby facilitating the management of the encryption key. Further, 10 a security of the authorization information is kept by the identification information peculiar to the content user, and a fraudulent use of the digital content can be prevented. Moreover, the authorization information is integrally embedded into the encrypted content, and hence the procedure 15 of transferring and receiving the key is simplified, which might eliminate a possibility of the key for decrypting the encrypted content being lost or broken and is no time-consuming of reissuing the key.

Other Embodiments

20 (A) The recording medium, stored with the synthesized data obtained by the content user 2, on which the synthesized data is decrypted and developed, may include, in addition to the hard disk, an MO, a ZIP, a DVD, an IC memory and those in other forms. In that case, IDs of those 25 devices may be used as the user information 14.

(B) Further, in the case of such a mode that the digital content is recorded on the recording medium such as the CD-ROM and the DVD and thus distributed, a content ID and a medium identification number written within a package may also be used as the user information 14.

(C) The system may also be constructed in such a way that the authorization information embedded into the watermarked sample data 47 contains a data field for recording the number of times with which the content user 2 decrypts and uses the digital content. In this case, if trying to use the content over a predetermined number of times, the system can be contrived to regulate this action. The system may also be constructed so that the number of times to use the content is updated when reading and 15 decrypting the encrypted content or when finishing the use of the digital content, and, with this updated number serving as invisible information, the watermarked sample data 47 is rewritten.

(D) The system may be constructed in such a manner
20 that the authorization information embedded into the
watermarked sample data 47 contains a data field for
recording the user information 14. In this case, an illicit
copy of the digital content and a fraudulent circulation
thereof can be prevented.

and the key separately, and therefore it never happens that the key for decrypting the substantive data file is lost, with no time-consuming process of reissuing the key.

The authorization information is embedded as the
5 invisible information into the sample data, and hence high security is maintained.

While only selected embodiments have been chosen to illustrate the present invention, to those skilled in the art it will be apparent from this disclosure that various
10 changes and modifications can be made herein without departing from the scope of the invention as defined in the appended claims. Furthermore, the foregoing description of the embodiments according to the present invention is provided for illustration only, and not for the purpose of
15 limiting the invention as defined by the appended claims and their equivalents.

What is claimed is:

1 1. A data management method comprising:
2 preparing a substantive data unit by encrypting digital
3 content that is for distribution;
4 extracting a portion of the digital content as sample
5 data, and preparing a sample data unit wherein authorization
6 information containing information for a content key
7 employed as an encryption key when encrypting the digital
8 content is embedded as invisible information; and
9 preparing synthesized data wherein the substantive data
10 unit and the sample data unit are synthesized, and
11 distributing the synthesized data.

1 2. The data management method set forth in claim 1,
2 wherein use is enabled by separating the authorization
3 information from the sample data unit, restoring the content
4 key for decrypting the substantive data unit from said
5 authorization information, and employing the content key to
6 decrypt the substantive data unit into the original digital
7 content.

1 3. The data management method set forth in claim 1, the
2 sample data being image data wherein at least one process
3 among image processing, resizing, compressing and a γ -
4 compensation is executed on image data contained in the
5 digital content.

1 4. The data management method set forth in claim 1,
2 wherein the sample data is index data for representing the
3 substantive data unit.

1 5. The data management method set forth in claim 4,
2 wherein the synthesized data contains a plurality of
3 substantive data units based on a plurality of digital
4 content items, and contains a plurality of sample data units
5 corresponding to the plurality of substantive data units;
6 and wherein sample data constituting the plurality of sample
7 data units is linked with respective corresponding ones of
8 the plurality of substantive data units.

1 6. The data management method set forth in claim 1,
2 wherein the sample data units are data structuralized in one
3 of JPEG and MPEG formats, and

4 the synthesized data is prepared by add-on synthesizing
5 the substantive data unit to the sample data unit using the
6 format of the sample data unit.

1 7. The data management method set forth in claim 1, the
2 authorization information being information wherein the
3 content key is encrypted, with the encryption key being at
4 least one of user identification information, equipment
5 identification information loaded in user-employed
6 computers, CPU identification information loaded in user-
7 employed computers, and identification information unique to
8 digital-content-storing recording media.

1 8. The data management method set forth in claim 1, the
2 authorization information being information wherein the
3 content key is encrypted, with the encryption key being
4 identification information common to a plurality of users.

1 9. The data management method set forth in claim 1, the
2 authorization information being information wherein the
3 content key is encrypted, with the encryption key being at
4 least one of identification information unique to
5 distributors of the digital content, and identification
6 information unique to authors of the digital content.

1 10. The data management method set forth in claim 7,
2 wherein a decryption key for decrypting the encrypted
3 content key is in common with the encryption key for
4 encrypting, being a shared key based on exclusive
5 information transmitted and received among users and content
6 distributors, using symmetric cryptography.

1 11. The data management method set forth in claim 8,
2 wherein a decryption key for decrypting the encrypted
3 content key is in common with the encryption key for
4 encrypting, being a shared key based on exclusive
5 information transmitted and received among users and content
6 distributors, using symmetric cryptography.

1 12. The data management method set forth in claim 9,
2 wherein a decryption key for decrypting the encrypted
3 content key is in common with the encryption key for

4 encrypting, being a shared key based on exclusive
5 information transmitted and received among users and content
6 distributors, using symmetric cryptography.

1 13. The data management method set forth in claim 7,
2 wherein the digital content distributors encrypt the content
3 key employing a secret key, and the users decrypt the
4 encrypted content key employing a public key provided in
5 advance from the digital content distributors, using public-
6 key cryptography.

1 14. The data management method set forth in claim 8,
2 wherein the digital content distributors encrypt the content
3 key employing a secret key, and the users decrypt the
4 encrypted content key employing a public key provided in
5 advance from the digital content distributors, using public-
6 key cryptography.

1 15. The data management method set forth in claim 9,
2 wherein the digital content distributors encrypt the content
3 key employing a secret key, and the users decrypt the
4 encrypted content key employing a public key provided in
5 advance from the digital content distributors, using public-
6 key cryptography.

1 16. The data management method set forth in claim 1,
2 wherein the sample data unit comprises as invisible
3 information a use count of times a user has used the digital

4 content; characterized in that the invisible information is
5 rewritten each time a user uses the digital content.

1 17. The data management method set forth in claim 1,
2 wherein the sample data unit comprises as invisible
3 information authorization information to enable use count
4 control; characterized in that the invisible information is
5 rewritten when a user uses the digital content a
6 predetermined number of times and more.

1 18. The data management method set forth in claim 16,
2 characterized in that the invisible information is rewritten
3 on decrypting and reading the substantive data unit.

1 19. The data management method set forth in claim 16,
2 characterized in that the invisible information is rewritten
3 when use of the digital content is ended.

1 20. The data management method set forth in claim 17,
2 characterized in that the invisible information is rewritten
3 on decrypting and reading the substantive data unit.

1 21. The data management method set forth in claim 17,
2 characterized in that the invisible information is rewritten
3 when use of the digital content is ended.

1 22. The data management method set forth in claim 16,
2 wherein the invisible information in the sample data unit
3 comprises an error recovery function by containing redundant
4 information.

1 23. The data management method set forth in claim 16,
2 characterized in that limits on read-out and use in
3 decrypting the substantive data unit are governed based on
4 the invisible information in the sample data unit.

1 24. The data management method set forth in claim 16,
2 characterized in that one of year, month, date, and time
3 limits within which read-out and use is possible in
4 decrypting the substantive data unit are governed based on
5 the invisible information in the sample data unit.

ABSTRACT

A data management method that by encrypting and distributing digital content prevents copyright infringement, and that prevents authorization information for decrypting the encrypted digital content from being damaged or otherwise lost. Encrypted content 45 is prepared by encrypting digital content 11 with a content key 44. A portion of the digital content 11 is extracted as sample data 41. A secret key 46, by which the content key 44 is encrypted with user information 14, is embedded as invisible information into the sample data 41, thus preparing watermarked sample data 47. The watermarked sample data 47 is synthesized with the encrypted content 45 to form synthesized data 48. The synthesized data 48 is distributed.

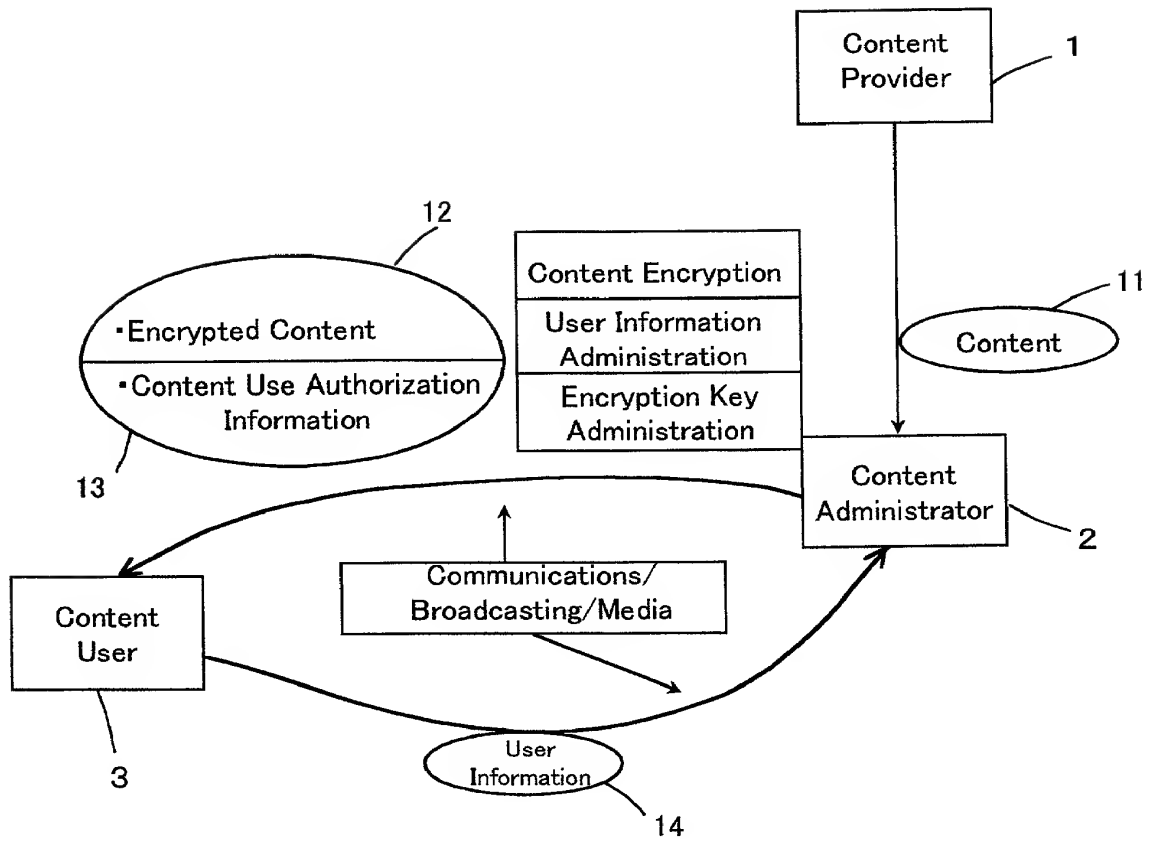
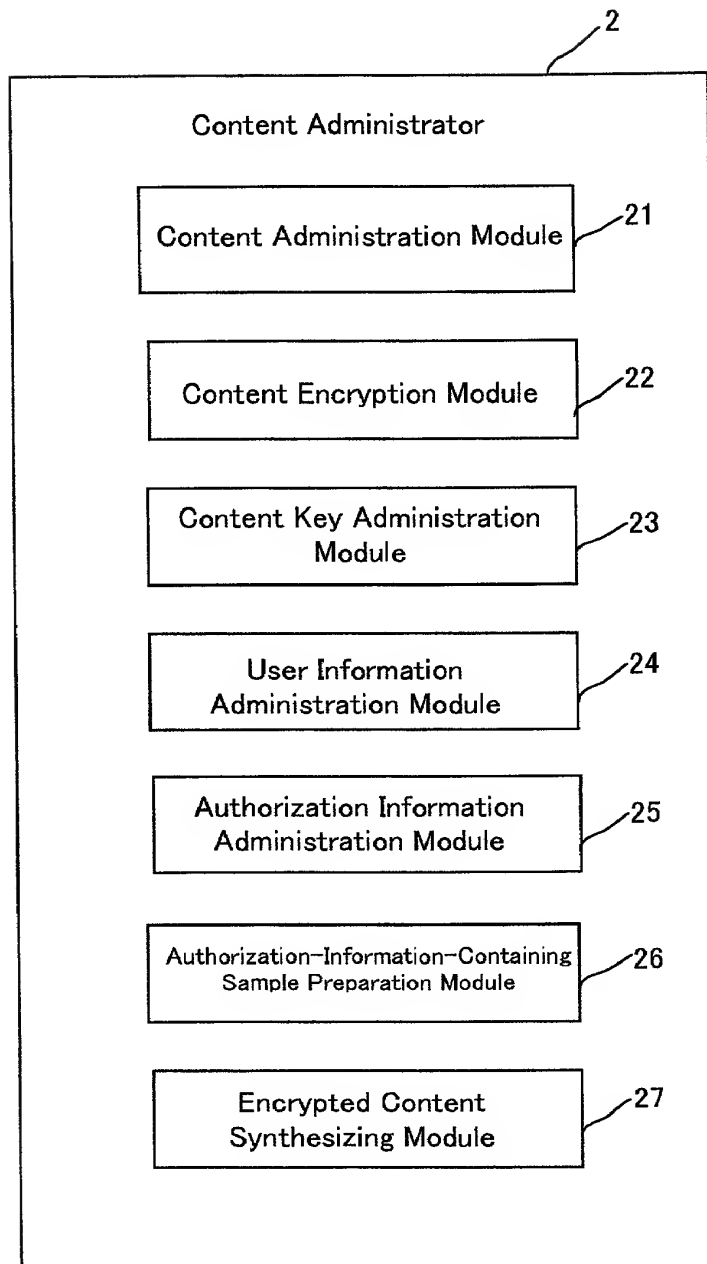


Fig. 1



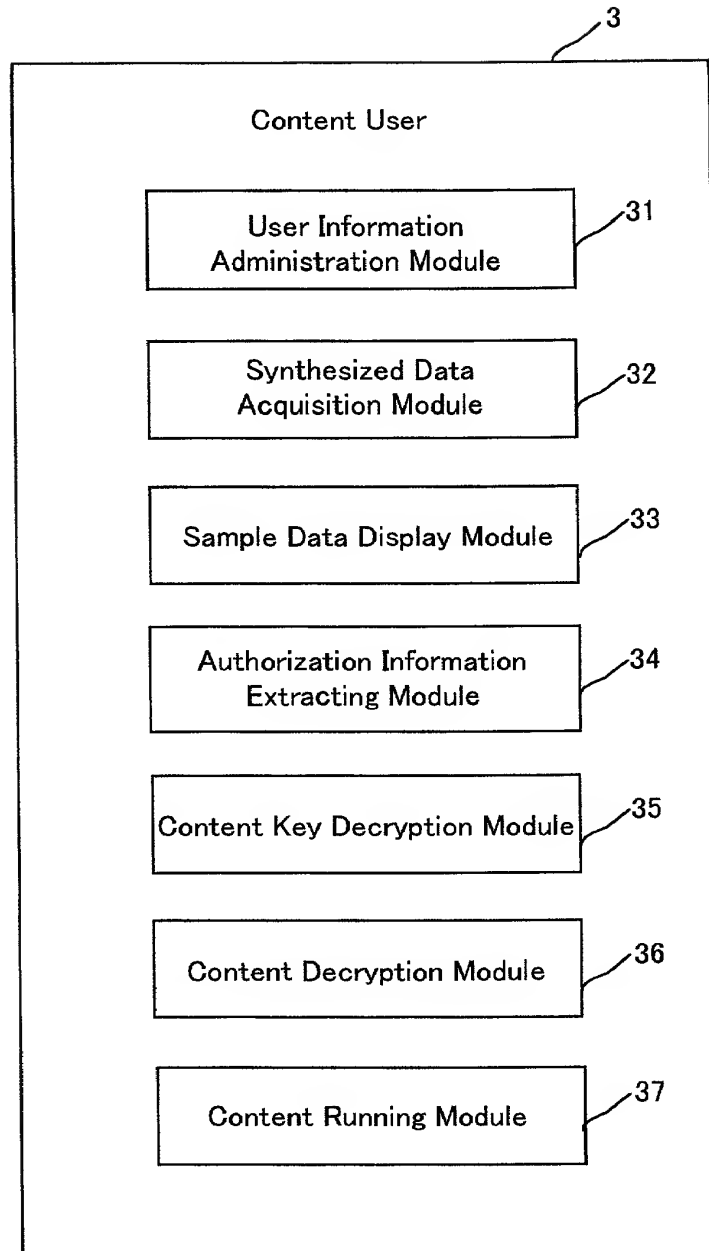


Fig. 3

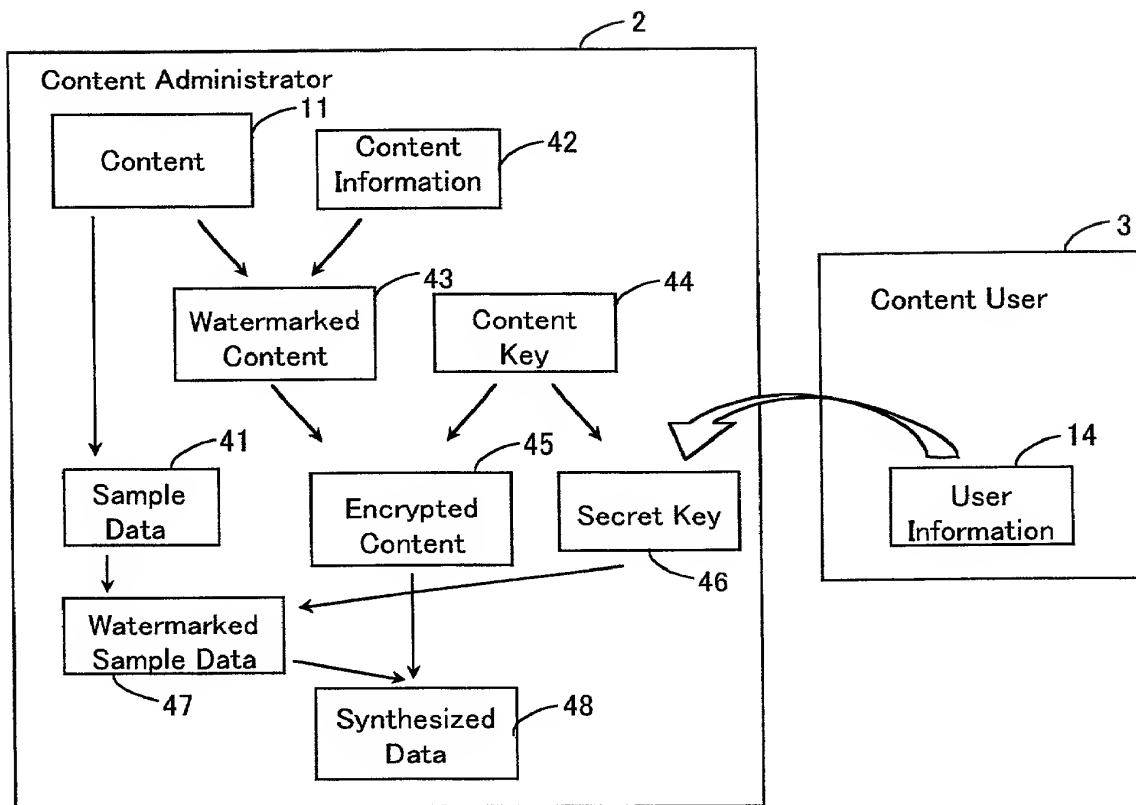


Fig. 4

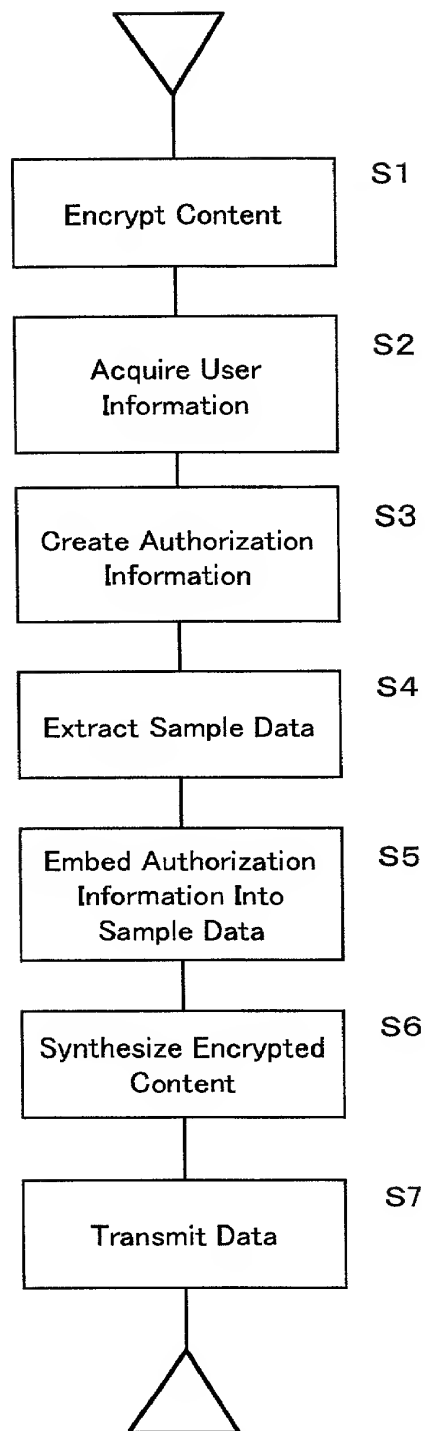


Fig. 5

Fig. 6

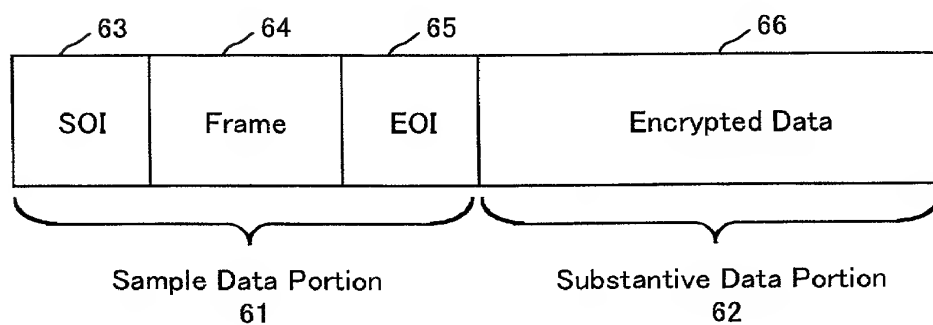
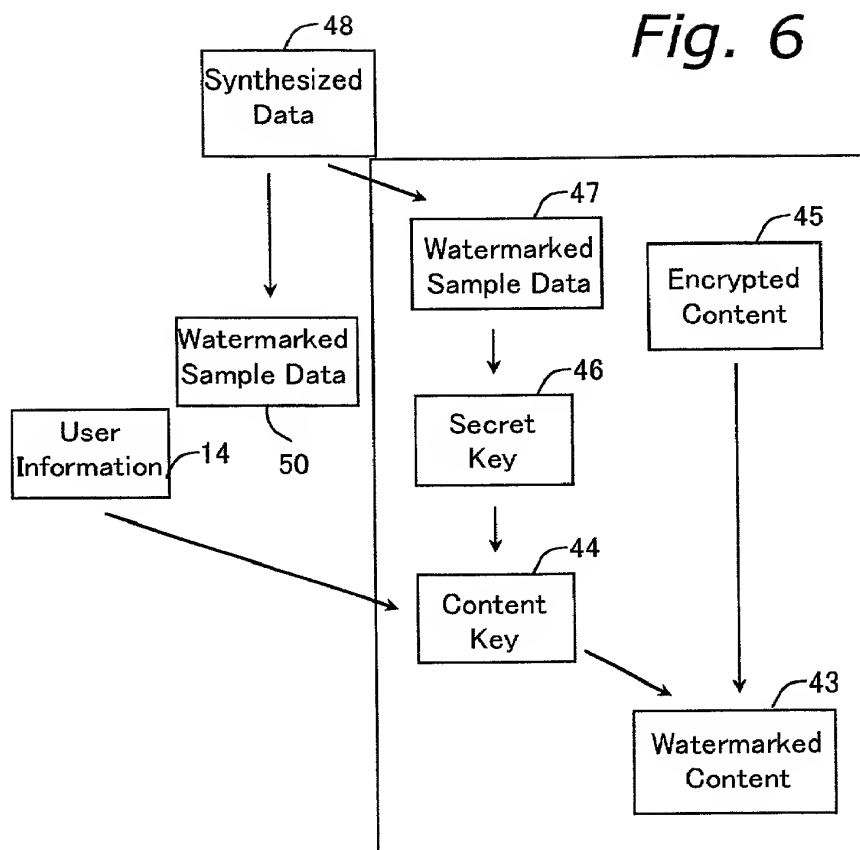


Fig. 8

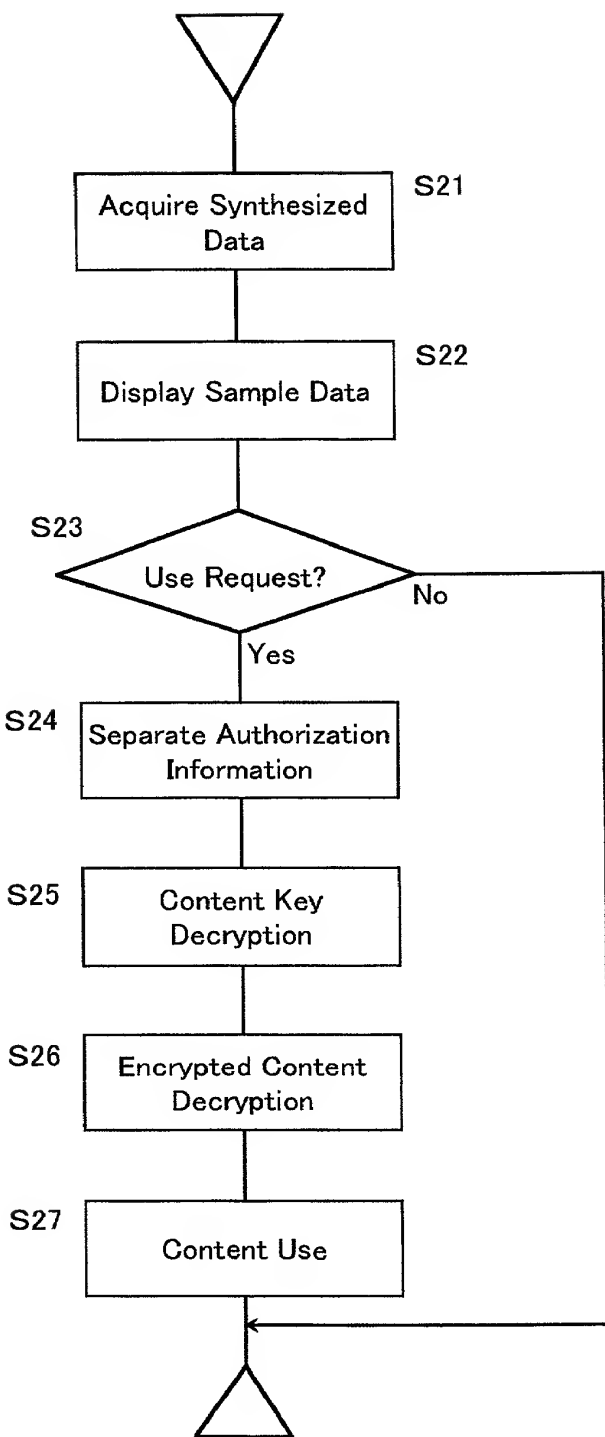


Fig. 7

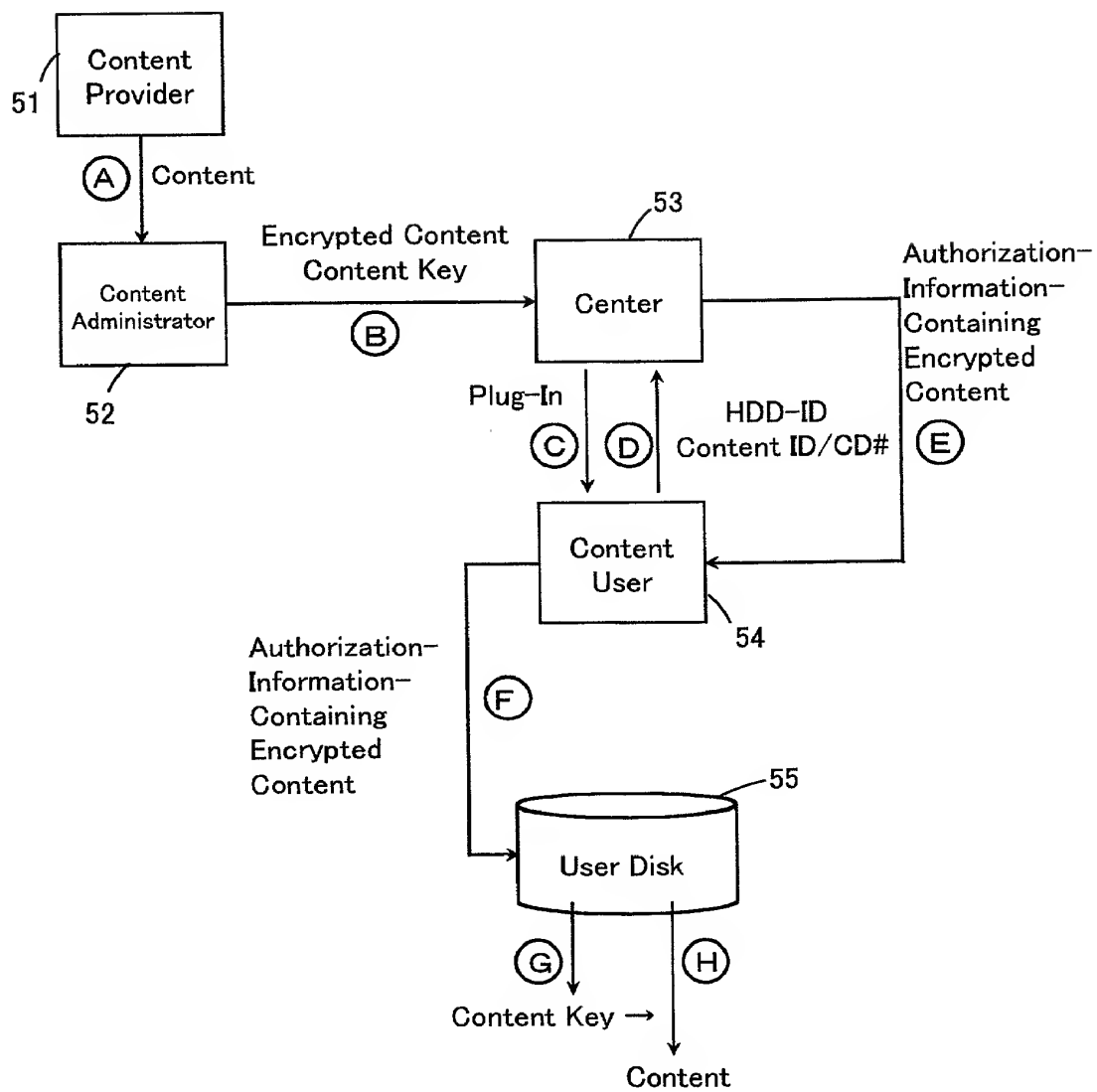


Fig. 9

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Declaration and Power of Attorney For Patent Application

特許出願宣言書及び委任状

Japanese Language Declaration

日本語宣言書

下記の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DATA MANAGEMENT METHOD

上記発明の明細書（下記の欄でx印がついていない場合は、本書に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ 月 日 に提出され、米国出願番号または特許協定条約国際出願番号を _____ とし、
（該当する場合） _____ に訂正されました。

☐ was filed on _____
as United States Application Number or
PCT International Application Number
_____ and was amended on
_____ (if applicable).

私は、特許請求範囲を含む上記訂正後の明細書を検討し、内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、連邦規則法典第37編第1条56項に定義されるとおり、特許資格の有無について重要な情報を開示する義務があることを認めます。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基づき下記の、米国外の国の少なくとも一カ国を指定している特許協力条約365(a)項に基づく国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

外国での先行出願

11-147769

(Number)
(番号)

Japan

(Country)
(国名)

(Number)
(番号)

(Country)
(国名)

私は、第35編米国法典119条(e)項に基づいて下記の米国外の特許出願規定に記載された権利をここに主張いたします。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

私は、下記の米国法典第35編120条に基づいて下記の米国外の特許出願に記載された権利、又は米国を指定している特許協力条約365条(c)に基づき権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国外の特許出願に開示されていない限り、その先行米国外出願書提出日以降で本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1条56項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

私は、私自身の知識に基づいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じることに基づく表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行為は米国法典第18編第1001条に基づき、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の声明を行なえば、出願した、又は既に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby claim foreign priority under Title 35, United States Code, Section 119 (a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Priority Not Claimed

優先権主張なし

27/05/99

(Day/Month/Year Filed)
(出願年月日)

(Day/Month/Year Filed)
(出願年月日)

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below.

(Application No.)
(出願番号)

(Filing Date)
(出願日)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of application.

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration
(日本語宣言書)

委任状： 私は下記の発明者として、本出願に関する一切の手続きを米特許商標局に対して遂行する弁理士または代理人として、下記の者を指名いたします。(弁理士、または代理人の氏名及び登録番号を明記のこと)

James D. Halsey, Jr., 22,729; Harry John Staas, 22,010; David M. Pitcher, 25,908; John C. Garvey, 28,607; J. Randall Beckers, 30,358; William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D. Stein, 37,240; Paul I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Marlette, 35,269; Harlan B. Williams, Jr., 34,756; George N. Stevens, 36,938; Michael C. Soldner, 41,455; Norman L. Ourada, 41,235; Kevin R. Spivak, P-43,148; and William M. Schertler, 35,348 (agent)

書類送付先

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number)

Send Correspondence to:

STAAS & HALSEY
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001

直接電話連絡先： (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY
(202) 434-1500

唯一または第一発明者名

Full name of sole or first inventor

Hideyuki HIRANO

発明者の署名

日付

Inventor's signature

Date

Hideyuki Hiranori April 21, 2000

住所

Residence

c/o FUJITSU LIMITED

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, Japan

国籍

Citizenship

Japan

私書箱

Post Office Address

Same as above

第二共同発明者

Full name of second joint inventor, if any

Seigo KOTANI

第二共同発明者

日付

Second inventor's signature

Date

Seigo Kotani April 21, 2000

住所

Residence

c/o FUJITSU LIMITED

1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, Japan

国籍

Citizenship

Japan

私書箱

Post Office Address

Same as above

(第三以降の共同発明者についても同様に記載し、署名をすること)

(Supply similar information and signature for third and subsequent joint inventors.)

Japanese Language Declaration

	Full name of third joint inventor, if any Shinji HASHIMOTO	
日付	Third Inventor's signature <i>Shinji Hashimoto</i>	Date April 21, 2000
住所 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, Japan	Residence C/O FUJITSU LIMITED	
国籍	Citizenship Japan	
郵便の宛先	Post Office Address Same as above	

	Full name of fourth joint inventor, if any	
日付	Fourth Inventor's signature	Date
住所	Residence	
国籍	Citizenship	
郵便の宛先	Post Office Address	

	Full name of fifth joint inventor, if any	
日付	Fifth Inventor's signature	Date
住所	Residence	
国籍	Citizenship	
郵便の宛先	Post Office Address	

	Full name of sixth joint inventor, if any	
日付	Sixth inventor's signature	Date
住所	Residence	
国籍	Citizenship	
郵便の宛先	Post Office Address	

(第六またはそれ以降の共同発明者に対しても同様な情報および署名を提供すること。)

(Supply similar information and signature for third and subsequent joint inventors.)